Need-Based Network Traffic Collection

Nathan Dell and Angela Horneman

Report Documentation Page		*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE **15 FEB 2015**	2. REPORT TYPE **N/A**	3. DATES COVERED
4. TITLE AND SUBTITLE **Need Based Network Traffic Collection**		5a. CONTRACT NUMBER
		5b. GRANT NUMBER
		5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) **Horneman /Angela**		5d. PROJECT NUMBER
		5e. TASK NUMBER
		5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213**		8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)
12. DISTRIBUTION/AVAILABILITY STATEMENT **Approved for public release, distribution unlimited.**		
13. SUPPLEMENTARY NOTES **The original document contains color images.**		
14. ABSTRACT		
15. SUBJECT TERMS		

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**SAR**	**14**	

Background
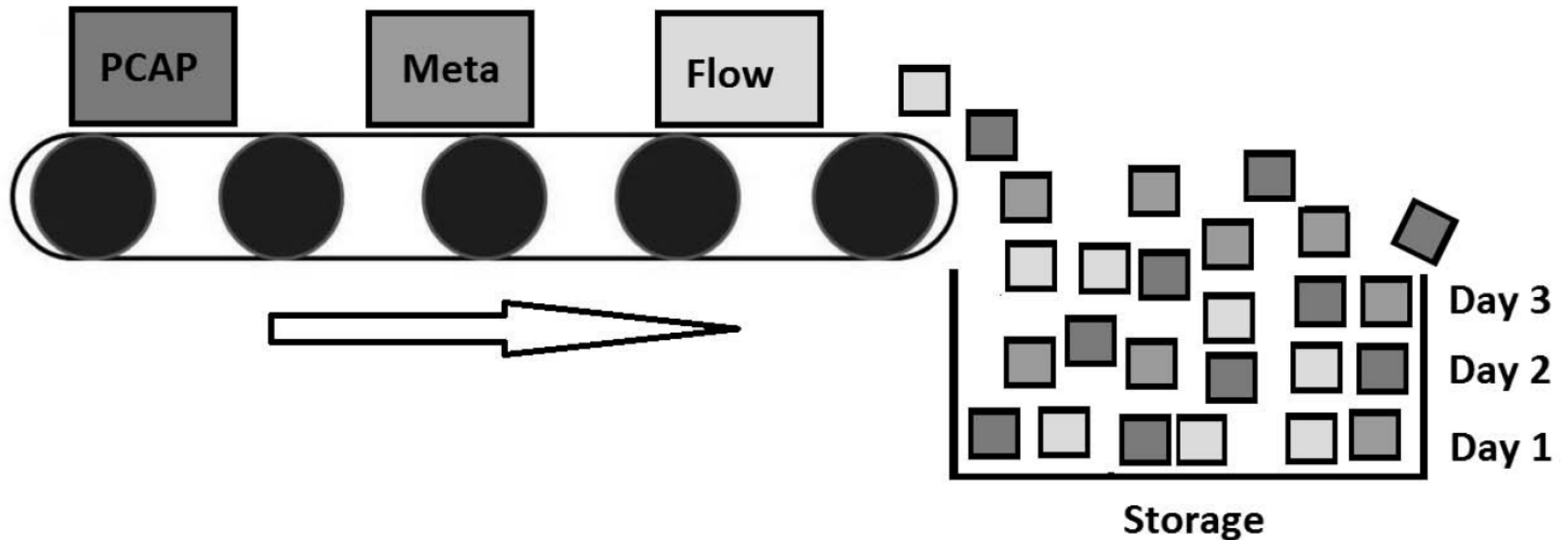
Network traffic monitoring is important.

Storage is important.

Analysis is important.

The Problem

"Collect everything mentality" is not effective.

- Network data typically rolls off before it becomes useful to analysts

- Some data collected has little to no value ever.

- Too much data inhibits analysis.

- Storage can become expensive.

When you can't keep everything, what do you do?

The Solution

A methodology to help organizations to collect

- the right network information
- at the right tiers
- for the right amount of time

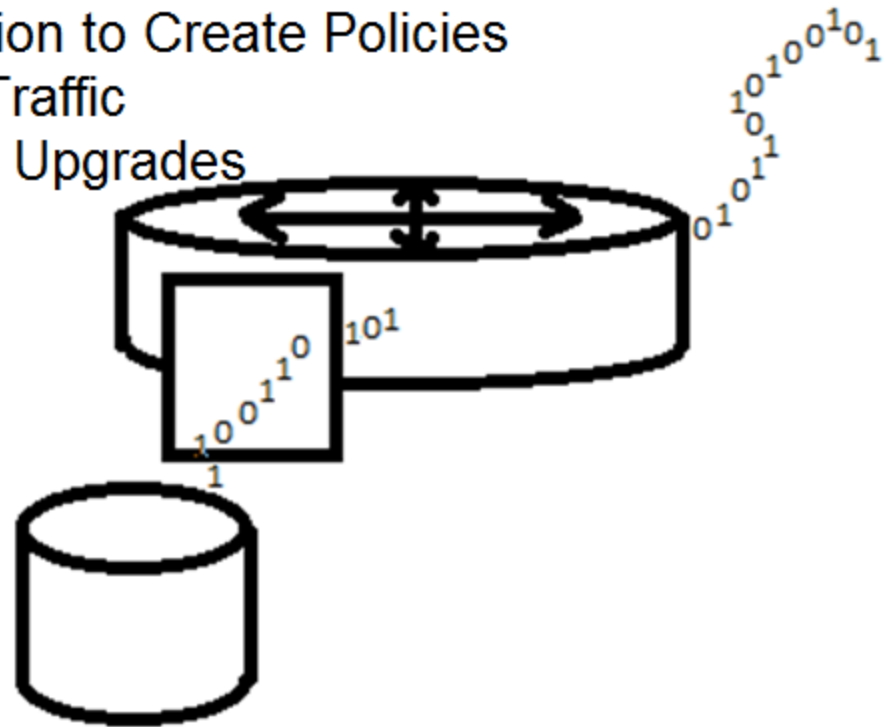[Smart Collection and Storage Method for Network Traffic Data](http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=304860)

Available online in the SEI Digital Library

http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=304860

Why do I need this?

- ✓ Investigate Attacks
- ✓ Enforce Policies
- ✓ Provide Information to Create Policies
- ✓ Profile Network Traffic
- ✓ Plan for Network Upgrades
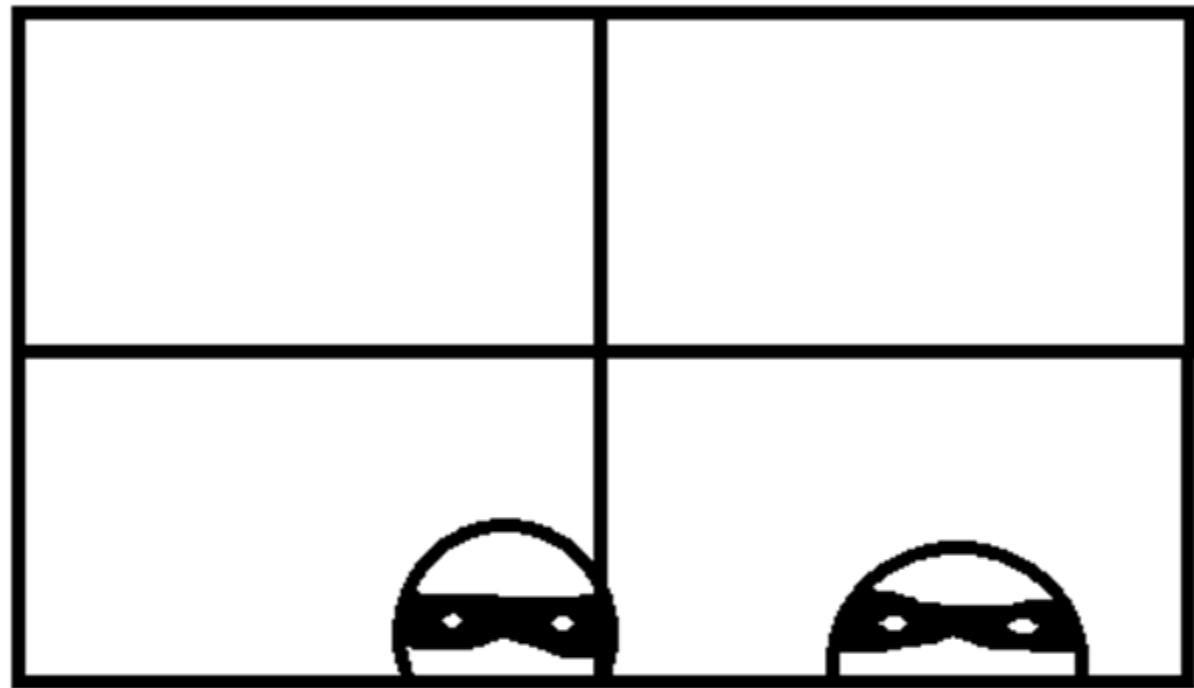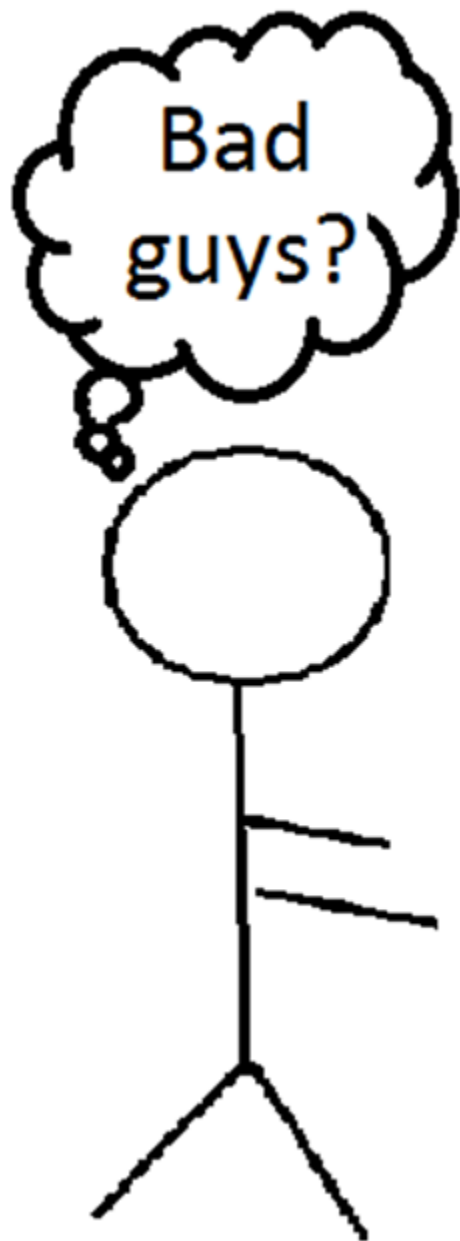
Scanning
Indexing
Malware Drop #1
C2/Backdoor Comms #3
Worm Propagation #4
System Control #5
Exfiltration #2
Data Corruption #6
DoS/DDoS Floods #8
DoS/DDoS Crashes #7

TCP: Encrypted
TCP: HTTP
TCP: Remote Connections
TCP: Email
TCP: File Copy
TCP: VoIP
TCP: All other TCP
UDP: Encrypted
UDP: DNS
UDP: Remote Connections
UDP: VoIP
UDP: All other UDP
ICMP
Other
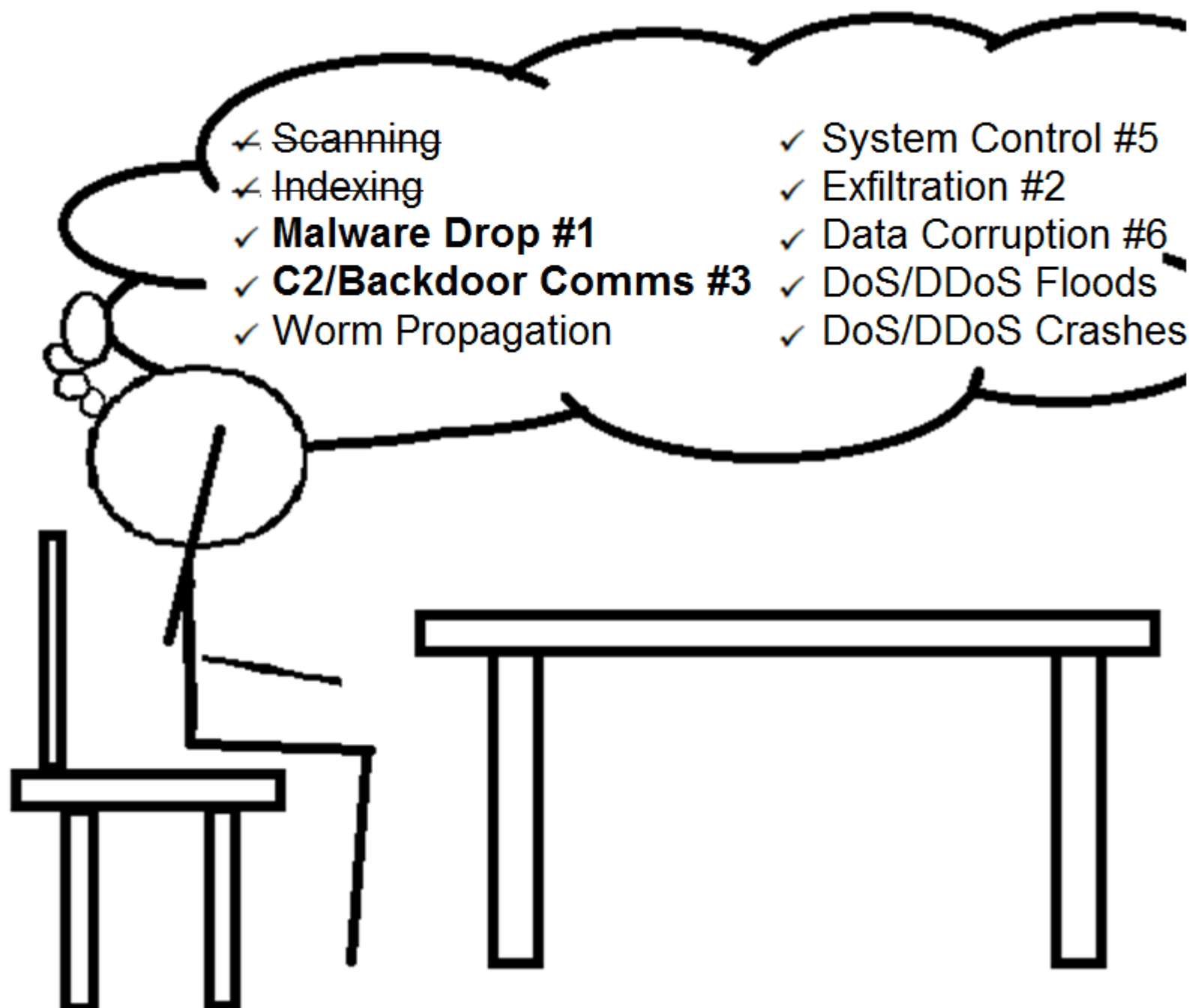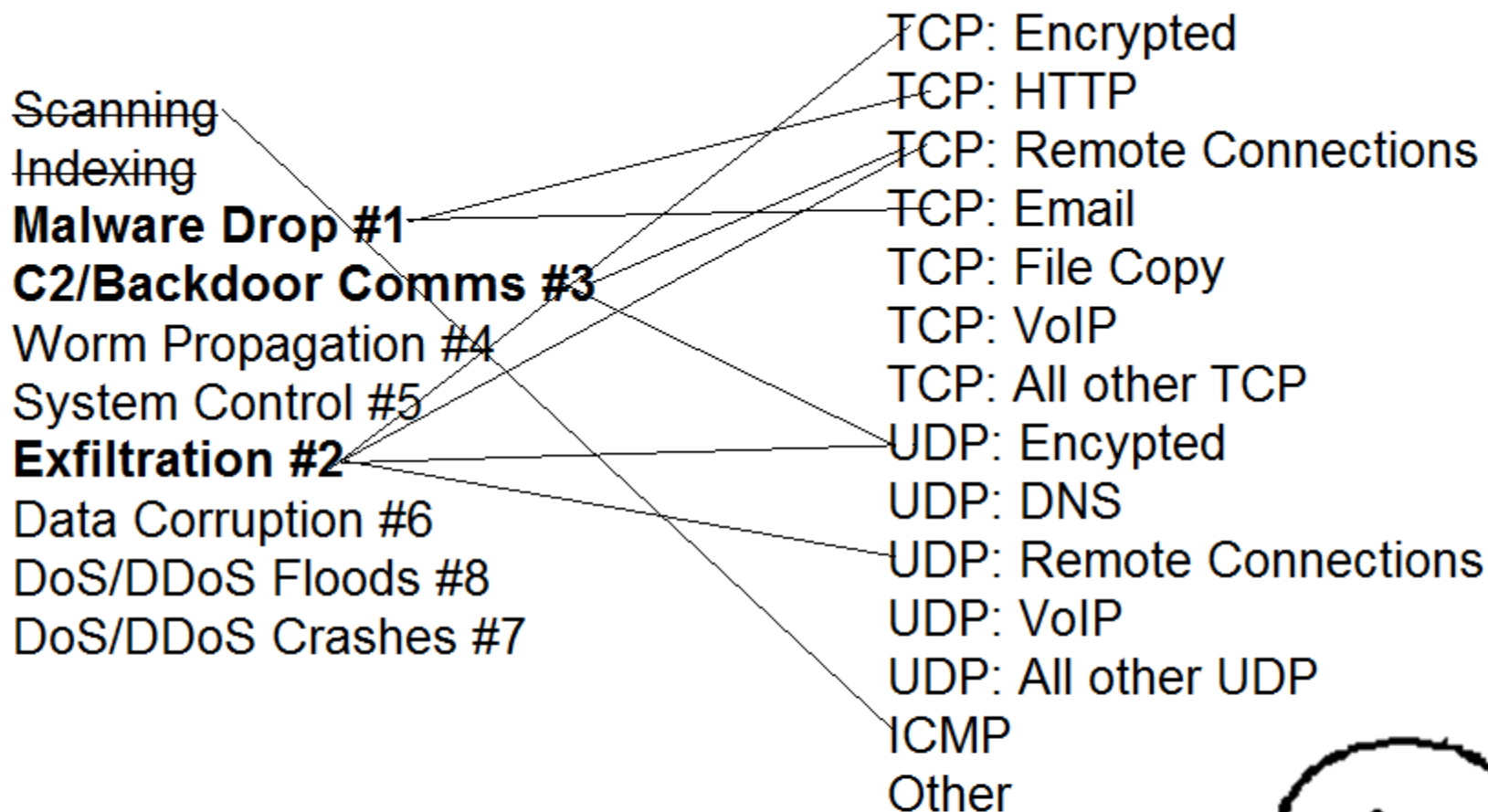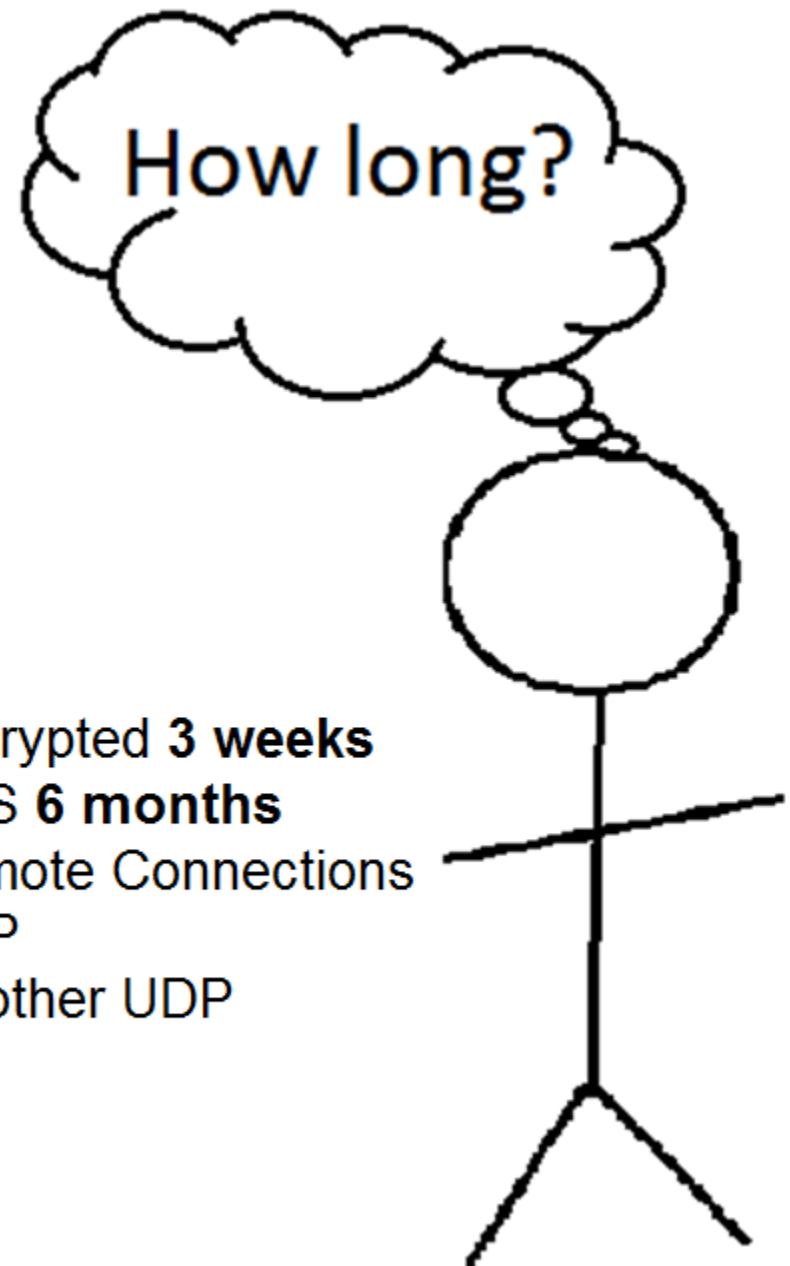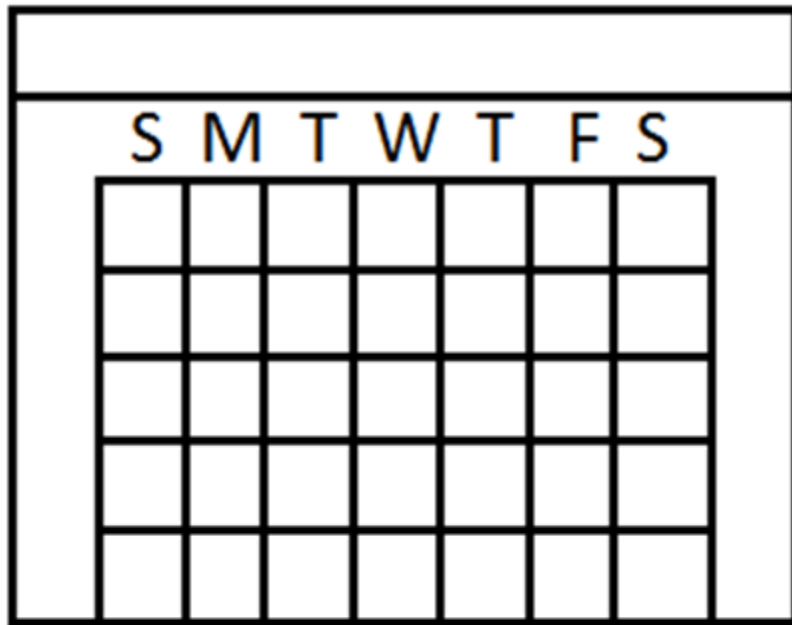
TCP: Encrypted **3 weeks**   UDP: Encrypted **3 weeks**
TCP: HTTP **6 months**   UDP: DNS **6 months**
TCP: Remote Connections   UDP: Remote Connections
TCP: Email **2 years**   UDP: VoIP
TCP: File Copy   UDP: All other UDP
TCP: VoIP   ICMP
TCP: All other TCP   Other
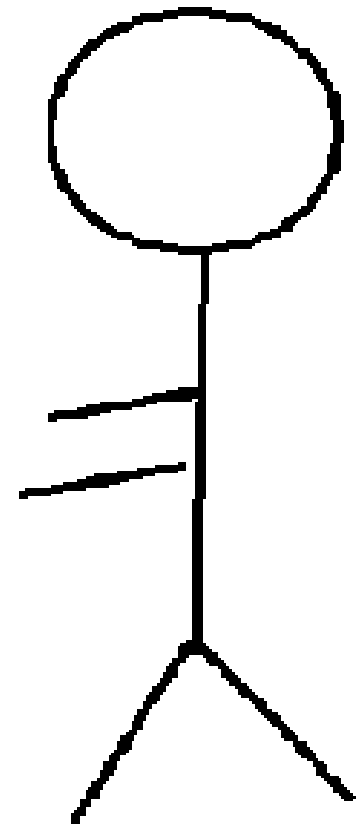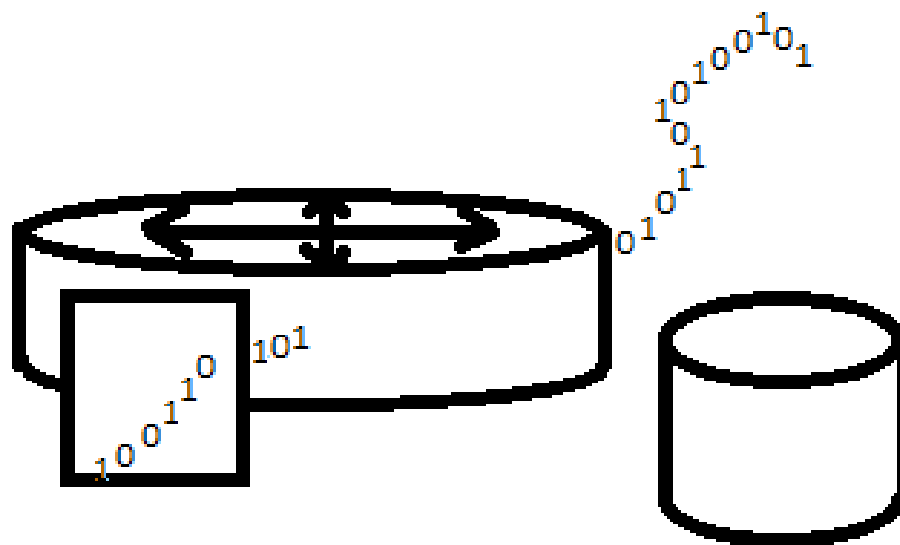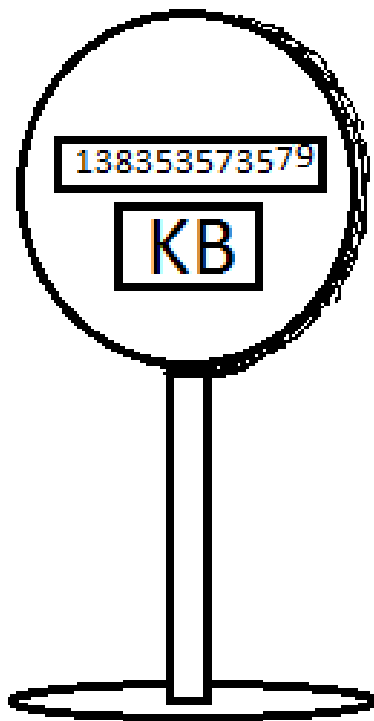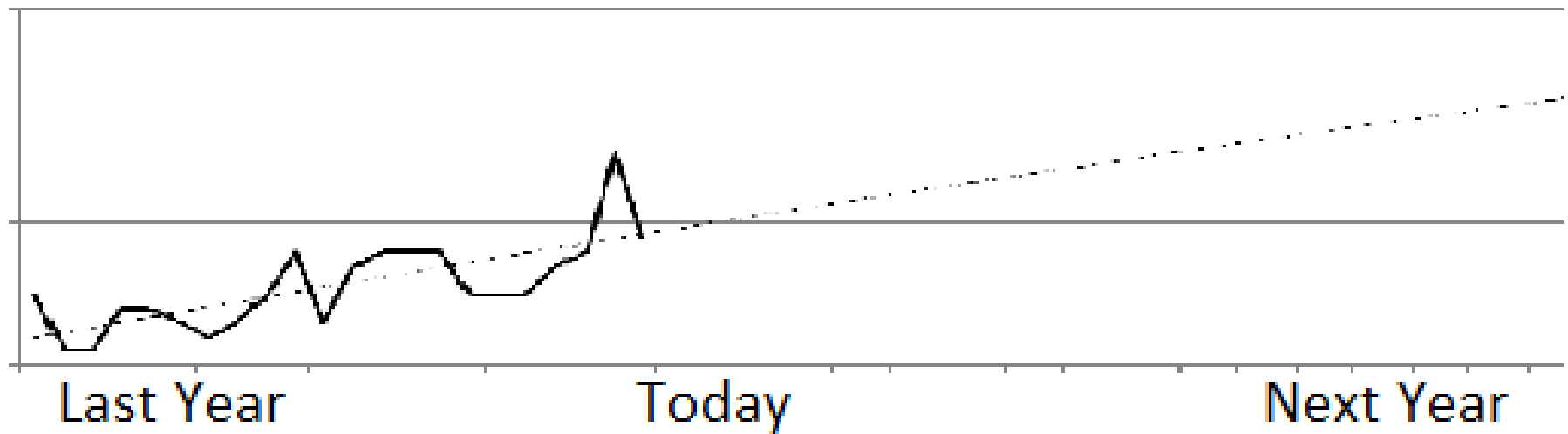
Application of the Methodology

$$\text{Current Storage } X \left((1 + \text{Growth Rate})^{Months} \left(\frac{ending\ value}{starting\ value}\right)^{\left(\frac{1}{\#\ months}\right)} - 1 \right.$$

	Monthly Growth Rates				Storage per Day in 24 Months: All			Storage per Day in 24 Months: Peak		
	All Traffic (Bytes)	Peak Traffic (Bytes)	All Traffic (Flows)	Peak Traffic (Flows)	N (in GBs)	A (in GBs)	P (in TBs)	N (in GBs)	A (in GBs)	P (in TBs)
TCP: HTTP	0.92%	2.47%	0.92%	2.47%	292.7	443.3	223.9	351.4	532.3	268.9
TCP: Encrypted HTTP	0.92%	2.47%	0.92%	2.47%	154.0	~~233.3~~	~~128.1~~	184.9	~~280.2~~	~~153.9~~
TCP: VoIP	0.61%	3.41%	0.61%	2.16%	0.0	0.0	~~0.0~~	0.0	0.1	~~0.0~~
UDP: VoIP	0.92%	2.47%	0.92%	2.47%	2.9	4.3	~~0.0~~	3.4	5.2	~~0.1~~
UDP: Encrypted VoIP	0.61%	1.85%	0.61%	1.85%	0.0	0.1	~~0.0~~	0.0	0.1	~~0.0~~
				Unfiltered:		~~1225.3~~	~~603.1~~		~~1494.0~~	~~728.6~~
				Filtered:	808.8	978.3	469.1	982.3	1197.4	567.5

Questions?

Angela Horneman

ahorneman@cert.org

Nathan Dell

nathand@cert.org

Software Engineering Institute | Carnegie Mellon University.